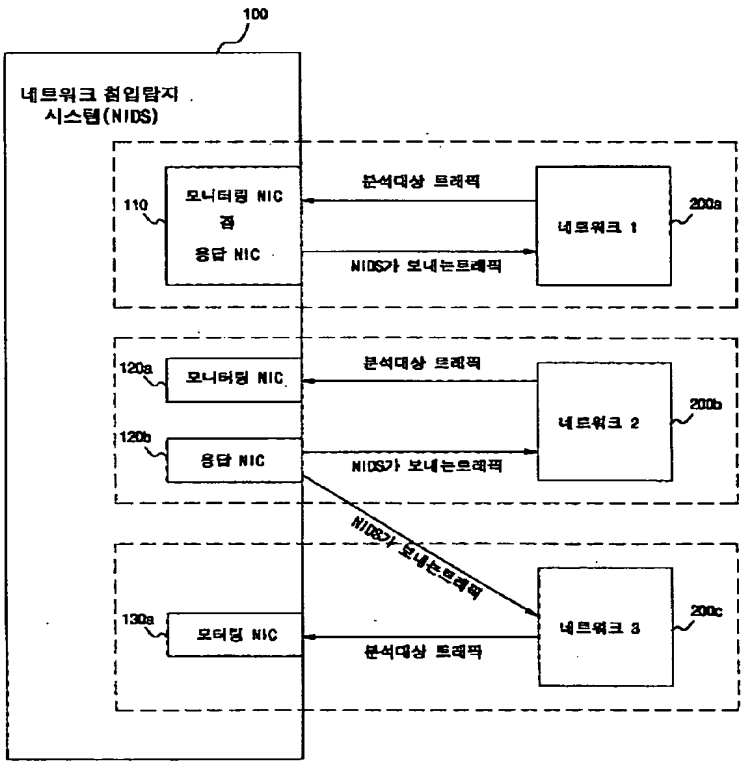
KOREAN PATENT ABSTRACTS(KR)

Document Code:A
(11) Publication No.1020020088956 (43) Publication.Date. 20021129
(21) Application No.1020010028052 (22) Application Date. 20010522
(51) IPC Code:
H04L 12/22

(71) Applicant:
INZEN CO., LTD.
(72) Inventor:
HAN, DONG HUN
(30) Priority:

(54) Title of Invention
NETWORK BASED INTRUSION DETECTION SYSTEM

Representative drawing



(57) Abstract:

PURPOSE: A network based intrusion detection system is provided to actively block and disturb the attempt of hacking irrespective of the configuration of a network when network intrusion such as hacking, service attack, and scanning is sensed.

CONSTITUTION: A monitoring NIC(Network Interface Card) and response NIC(110) collects a packet of an analyzing object traffic from a network 1(200a), and transmits a packet for performing an SNA(Suspicious Network Activity) and a session kill to the network 1(200a). A monitoring NIC(120a) collects a packet of an analyzing object traffic from a network 2(200b), and a response NIC(120b) transmits a packet for performing an SNA and a session kill to the network 2 (200b). A monitoring NIC(130a) collects a packet of an analyzing object traffic from a

network 3(200c), and transmits a packet for performing the SNA and the session kill to the network 3(200c) through the response NIC(120b).

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.		(11) 공개번호	특2002-0088956
H04L 12/22		(43) 공개일자	2002년11월29일
(21) 출원번호	10-2001-0028052		
(22) 출원일자	2001년05월22일		

(71) 출원인 (주)인젠
대한민국
135-502
서울 강남구 대치3동 996-17 미래에셋벤처타워 B동 4 5층
(72) 발명자 한동훈
대한민국
463-060
경기도성남시분당구이매동140아름마을아파트516-1102
(74) 대리인 특허법인 엘엔케이

(77) 심사청구 있음

(54) 출원명 네트워크 침입탐지 시스템

요약

본 발명은 네트워크 침입탐지 시스템에 관한 것으로, 네트워크로부터 분석대상 트래픽의 패킷을 수집하는 모니터링(MN : Monitoring) NIC , 네트워크로 서스피셔스 네트워크 액티비티(SNA : Suspcious Network Activity)에 대한 대응 및 세션 킬(Session Kill)을 수행하기 위한 패킷을 보내는 응답(RN : Response) NIC을 구비하고, 더 나아가 여러개의 모니터링 NIC이 트래픽(Traffic) 분석을 수행하고 있을 경우, 여러개의 모니터링 NIC이 각각 응답 NIC을 하나씩 가지도록 상기 응답 NIC을 각각 따로 사용하거나 공유하도록 하며, 응답 NIC가 네트워크로 직접 패킷(Packet)을 보내지 못하는 상황인 경우, RN이 보내는 패킷에 대해 라우팅(Routing)을 수행 해 주는 응답 게이트웨이 (Response Gateway)도 사용할 수 있도록 함으로써 해킹이나 서비스 공격, 스캐닝 등의 네트워크 침입을 감지했을 때, 네트워크의 구성이 어떻게 되어 있는지에 상관없이 유연하게 해킹 시도에 대해 능동적으로 대처할 수 있어 해킹에 대해 적절히 조치하지 못하는 일을 최소화 할 수 있으며, 여러개의 네트워크를 감시해야 하는 상황하에서도 모든 기능이 정확하게 작동하도록 한 것이다.

대표도

도2

색인어

네트워크 침입탐지 시스템(NIDS), 네트워크 인터페이스 카드(NIC)

명세서

도면의 간단한 설명

도 1 은 포워딩만이 지원되는 L2 스위치를 사용한 전통적인 침입탐지 시스템의 구성도

도 2 는 본 발명에 따른 네트워크 침입탐지 시스템의 일 실시예를 도시한 구성도

도 3 은 본 발명에 따른 네트워크 침입탐지 시스템의 또 다른 실시예를 도시한 구성도

도 4 는 본 발명에 따른 네트워크 침입감시 시스템의 설정 프로그램 개요도

<도면의 주요부분에 대한 부호의 설명>

100 : 네트워크 침입탐지 시스템 110 : 인터페이스카드

120a, 130a : 모니터링 NIC 120b : 응답 NIC

200a : 네트워크1 200b : 네트워크2

200c : 네트워크3 300 : 응답 게이트웨이

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 네트워크 침입탐지 시스템에 관한 것으로, 특히, 네트워크에 흐르

는 모든 트래픽(Traffic)을 분석하여 위험하거나, 위험 가능성이 있는 행위들을 탐지하여 이를 차단하도록 하는 네트워크 침입탐지 시스템(NIDS : Network Based Intrusion Detection System)에 있어서의 네트워크 인터페이스 카드 구성에 관련되는 것이다.

네트워크 침입탐지 시스템(NIDS : Network Based Intrusion Detection System)은 네트워크에 흐르는 모든 트래픽(Traffic)을 분석하여 위험하거나, 위험 가능성이 있는 행위들을 탐지하여 이를 차단하고, 관리자에게 알리는 기능을 포함하는 시스템이다.

상기 차단은 크게 두 가지 경우로 나뉘며, 하나는 서스피셔스 네트워크 액티비티(SNA : Suspicious Network Activity)라 부르는 것으로, 취약점 분석, 네트워크 서비스 검색, 운영체제 종류 판단, 서비스 거부 공격 등 TCP/IP의 근본적인 취약점을 이용한 "로우 레벨 스캐닝/어택(Low Level Scanning/Attack)"에 대한 방해를 하는 경우이고, 다른 하나는 세션 킬(Session Kill)이라 부르는 것으로, 위험한 행위를 시도하는 TCP 연결을 강제로 끊는 것이다.

이 두가지는 모두 특정한 작용을 하도록 만들어진 네트워크 패킷(Packet)을 해당 네트워크 또는 호스트(Host)에 보내줌으로써 이루어진다.

따라서, 상기 네트워크 액티비티(SNA) 및 세션 킬(Session Kill) 모두 네트워크 침입탐지 시스템(NIDS)이 해당 네트워크 및 호스트에 패킷을 보낼 수 있어야만 이루어질 수 있다.

도 1 은 포워딩(Forwarding)만이 지원되는 L2 스위치를 사용하여 전통적인 침입탐지 시스템의 연결 양상을 도시한 것이다.

네트워크 침입탐지 시스템(NIDS)은 네트워크 인터페이스 카드(NIC : Network Interface Card)를 이용하여 네트워크로부터 패킷을 받아들여, 그 내용을 분석하고, 필요한 경우 패킷을 보내 특정 세션(Session)을 강제 종료 시키는 등의 작용을 하게 만들어진다.

도면에 도시한 네트워크 인터페이스 카드(NIC)는 상기 네트워크 침입탐지 시스템(NIDS)에 여러개 있을 수도 있다.

그러나, 네트워크 부분에 있는 장비의 한계 때문에 네트워크 인터페이스카드(NIC)가 네트워크로 패킷을 보낼 수 없는 경우에는 상기 네트워크 액티비티(SNA) 및 세션 킬(Session Kill)을 수행할 수 없다.

이러한 경우로는 네트워크 침입탐지 시스템(NIDS)에서 패킷(Packet) 수집용의 NIC (Monitoring NIC)을 연결한 네트워크 장비의 포트(Port)가 패킷(Packet)을 전달해 주는 방식이 미러링(Mirroring)이 아닌 포워딩(Forwarding)인 경우를 예를 들 수 있다.

이 때, 패킷을 받아들이는 네트워크 인터페이스카드(NIC)와 보내는 네트워크 인터페이스카드(NIC)가 같은 경우, 네트워크 침입탐지 시스템(NIDS)의 네트워크 인터페이스카드(NIC)로부터 네트워크상의 포워딩(Forwarding)이 설정된 포트(Port)로 패킷을 보내게 되고, 그 패킷이 실제로 네트워크에 도달하지 못하여 능동적 대응 방식을 취하지 못한다.

발명이 이루고자 하는 기술적 과제

본 발명은 상기와 같은 문제점을 해결하기 위하여 발명된 것으로, 네트워크 관련 하드웨어의 한계를 극복하여 해킹이나 서비스 공격, 스캐닝 등의 네트워크 침입을 감지했을 때, 네트워크의 구성이 어떻게 되어 있는지에 상관없이 해킹 시도에 대한 차단 및 방해를 능동적으로 할 수 있는 네트워크 침입탐지 시스템(NIDS)을 제공함을 그 목적으로 한다.

본 발명의 또 다른 목적은 여러 개의 패킷(Packet) 수집용 NIC이 존재하더라도, 각각의 NIC이 적절한 응답 NIC를 가지며, 그 작용이 보장되도록 할 수 있는 네트워크 침입탐지 시스템(NIDS)을 제공하는 것이다.

발명의 구성 및 작용

상기와 같은 목적을 달성하기 위한 본 발명에 따른 네트워크 침입탐지 시스템의 일 양상에 따르면, 본 발명에 따른 네트워크 침입탐지 시스템은 네트워크에 흐르는 모든 트래픽(Traffic)을 분석하여 위험하거나, 위험 가능성이 있는 행위들을 탐지하여 이를 네트워크 액티비티(SNA) 및 세션 킬(Session Kill)을 수행하여 해킹을 차단 및 방지하는 네트워크 침입탐지 시스템(NIDS : Network Based Intrusion Detection System)에 있어서, 상기 네트워크 침입탐지 시스템(NIDS)이 네트워크로부터 분석대상 트래픽의 패킷을 수집하는 모니터링 NIC과; 네트워크로 네트워크 액티비티(SNA) 및 세션 킬(Session Kill)을 수행하기 위한 패킷을 보내는 응답 NIC을; 포함하는 적어도 하나 이상의 제 1 형의 네트워크 인터페이스 카드를 포함하는 것을 특징으로 한다.

본 발명에 따른 네트워크 침입탐지 시스템의 부가적인 양상에 따르면, 본 발명에 따른 네트워크 침입탐지 시스템은 네트워크로부터 분석대상 트래픽의 패킷을 수집하는 모니터링 NIC 만으로 이루어진 적어도 하나 이상의 제 2 형의 네트워크 인터페이스 카드를 더 포함하는 것을 특징으로 한다.

본 발명에 따른 네트워크 침입탐지 시스템의 부가적인 양상에 따르면, 본 발명에 따른 네트워크 침입탐지 시스템의 상기 제 2 형의 네트워크 인터페이스 카드는 상기 제 1 형의 네트워크 인터페이스 카드의 응답 NIC 중 어느 하나를 공유하되, 해당 응답 NIC은 공유된 제 2 형의 네트워크 인터페이스 카드의 네트워크로의 응답에 대한 환경정보를 포함함에 의해 상기 제 2 형의 네트워크 인터페이스 카드의 모니터링 NIC이 수집한 패킷에 대한 응답 패킷을 상기 공유된 응답 NIC을 통해 네트워크로 보내는 것을 특징으로 한다.

본 발명에 따른 네트워크 침입탐지 시스템의 부가적인 양상에 따르면, 본 발명에 따른 네트워크 침입탐지 시스템은 상기 적어도 하나 이상의 응답 NIC으로부터 네트워크로 전송되는 네트워크 액티비티(SNA) 및 세션 킬(Session Kill)을 수행하기 위한 패킷들을 라우팅(Routing)하는 응답 게이트웨이(Gateway)를 더 포함하는 것을 특징으로 한다.

본 발명에 따른 네트워크 침입탐지 시스템의 부가적인 양상에 따르면, 본 발명에 따른 네트워크 침입탐지 시스템은 상기 제 1 형의 네트워크 인터페이스카드의 모니터링 NIC과 응답 NIC이 일체인 것을 특징으로 한다.

본 발명에 따른 네트워크 침입탐지 시스템의 부가적인 양상에 따르면, 본 발명에 따른 네트워크 침입탐지 시스템은 상기 제 1 형의 네트워크 인터페이스카드의 모니터링 NIC과 응답 NIC이 각각 분리되어 구성된 것을 특징으로 한다.

이하, 첨부된 도면을 참조하여 기술되는 본 발명의 바람직한 실시예를 통해 본 발명을 당업자가 용이하게 이해하고 재현할 수 있도록 상세히 설명한다.

도 2 는 본 발명에 따른 네트워크 침입탐지 시스템(NIDS)의 일 실시예를 도시한 것이다.

도면에 도시한 바와같이 이 실시예에서는 네트워크 침입탐지 시스템(100)은 3개의 침입탐지 모듈을 구비하고 있다.

이하, 네트워크로부터 분석대상 트래픽의 패킷을 수집하는 네트워크 인터페이스카드를 모니터링(MN : Monitoring) NIC , 네트워크로 네트워크 액티비티(SNA) 및 세션 킬(Session Kill)을 수행하기 위한 패킷을 보내는 네트워크 인터페이스카드를 응답 NIC (RN : Response NIC)이라 한다.

첫번째 모듈은 네트워크1(200a)로부터 분석대상 트래픽의 패킷을 수집하는 모니터링 NIC과, 네트워크1(200a)로 네트워크 액티비티(SNA) 및 세션 킬(Session Kill)을 수행하기 위한 패킷을 보내는 응답 NIC을 일체로 구성하여 하나의 인터페이스카드(110)를 통해 모니터링 NIC과 응답 NIC 역할을 겸비하도록 한 것이다.

즉, 이 모듈은 상기 네트워크1(200a)로부터 동일한 네트워크 인터페이스카드를 통해 분석대상 트래픽의 패킷을 수집하고, 동일한 네트워크 인터페이스 카드(110)를 통해 상기 네트워크1(200a)로 네트워크 액티비티(SNA) 및 세션 킬(Session Kill)을 수행하기 위한 패킷을 보낸다.

두번째 모듈은 네트워크2(200b)로부터 분석대상 트래픽의 패킷을 수집하는 모니터링 NIC(120a)과, 네트워크2(200b)로 네트워크 액티비티(SNA) 및 세션 킬(Session Kill)을 수행하기 위한 패킷을 보내는 응답 NIC(120b)을 별도로 구성한 것이다.

즉, 이 모듈은 상기 네트워크2(200b)로부터 모니터링 NIC(120a)을 통해 분석대상 트래픽의 패킷을 수집하고, 상기 모니터링 NIC(120a)과 별도로 구성한 응답 NIC(120b)를 통해 상기 네트워크2(200b)로 네트워크 액티비티(SNA) 및 세션 킬(Session Kill)을 수행하기 위한 패킷을 보낸다.

세번째 모듈은 네트워크3(200c)으로부터 분석대상 트래픽의 패킷을 수집하는 모니터링 NIC(130a)으로만 구성되고, 네트워크3(200c)로 네트워크 액티비티(SNA) 및 세션 킬(Session Kill)을 수행하기 위한 패킷을 보내는 응답 NIC(120b)을 상기 두번째 모듈과 공유하도록 구성한 것이다.

즉, 이 모듈은 상기 네트워크3(200c)으로부터 모니터링 NIC(130a)을 통해 분석대상 트래픽의 패킷을 수집하고, 상기 두번째 모듈의 응답 NIC(120b)를 통해 네트워크3(200c)으로 네트워크 액티비티(SNA) 및 세션 킬(Session Kill)을 수행하기 위한 패킷을 보낸다.

이 때, 상기 공유되는 응답 NIC(120b)은 상기 모니터링 NIC(130a)의 응답 방법에 대한 정보를 가지고 있어야 적절한 방법으로 패킷을 전송할 수 있다.

도 3 은 본 발명에 따른 네트워크 침입탐지 시스템(NIDS)의 또 다른 실시예를 도시한 것이다.

이 실시예에서는 응답 게이트웨이(300)를 사용하여 응답 패킷에 대한 라우팅(Routing)이 가능하도록 한 것이다.

즉, 이 경우에는 네트워크 침입탐지 시스템(100)의 응답 NIC으로부터 송출되는 네트워크 액티비티(SNA) 및 세션 킬(Session Kill)을 수행하기 위한 패킷을 응답 게이트웨이(300)를 통해 라우팅하여 네트워크로 전송함으로써 중간 단계의 네트워크에 NIC를 연결할 수 없는 상황이거나, 네트워크 상황이 좋지 않더라도, 라우터(Router)의 능력에 따라 응답이 가능하도록 한 것이다.

한편, 상기 네트워크 침입감지 시스템은 상기 각 모듈에 대해 모니터링 NIC과 응답 NIC을 짝지어 어떠한 방식으로 패킷을 보낼지를 결정하고, 결정된 방식에 따라 패킷을 보내기 위하여 필요한 정보들 예를들어, 패킷을 보내고자하는 곳의 공유되는 매체에 연결된 장치의 하드웨어 주소인 목적지의 MAC(Media Access Control) 어드레스를 수집한다.

설정 내용에 따라 어떤 응답 NIC을 통해 패킷을 보내게되는지를 결정하여 해당 목적지의 MAC 어드레스로 패킷을 보낸다.

이더넷(Ethernet) 환경하에서 패킷을 네트워크 침입감지 시스템으로부터 특정 호스트(Host)에 도달하게 하기 위해서는 목적지의 MAC 어드레스(Media Access Control Address)를 알아야만 한다.

이 맥(MAC) 어드레스는 다른 네트워크로 패킷을 보내기 위한 게이트웨이일 수도 있고, 같은 이더넷의 서브넷(Subnet)에 연결되어 있는 호스트의 MAC 어드레스 일 수도 있다.

또한, 응답 NIC이 보내는 패킷의 MAC 어드레스를 지정할 때도 비슷하게 IP 주소와 맞는 특정 호스트의 MAC 어드레스를 사용할 수 도 있고, 응답 NIC 자체의 MAC 어드레스일 수도 있다.

이 모든 것은 네트워크와 연결되어 있는 상태를 기준으로 판명해야 하기 때문에, 수동으로 네트워크 구성을 참고하여 설정하게 된다.

MAC 어드레스가 사용되는 유형을 나누어 보면, 출발지 MAC 어드레스(Source MAC Address)와 목적지 MAC 어드레스(Destination MAC Address)로 크게 나눌 수 있다. 출발지 MAC 어드레스는 패킷(Packet)을 보내는 NIC의 MAC 주소이고, 목적지 MAC 어드레스는 패킷(Packet)을 받는 NIC의 MAC 주소이다.

RN이 패킷(Packet)을 보낼 때 사용하는 출발지 MAC 어드레스는 3 가지로 나뉠 수 있다. 첫째는 원래의 MAC 어드레스를 사용하는 경우로, 이 경우는 (예를 들어) 더미 허브(Dummy Hub)에 연결되어 있는 경우이다. 더미 허브는 MAC 어드레스에 의해 아무런 영향을 받지 않기 때문에, IP 주소에 대응하는 MAC 어드레스를 사용하여도 상관이 없다. 따라서, 부작용이 전혀 없도록 원래의 MAC 어드레스를 사용하는 것이 가장 좋은 방법이다.

둘째는 자기 자신의 MAC 어드레스를 사용하는 경우로, 이 경우는 (예를 들어) L2 스위치에 연결되어 있을 경우이다. L2 스위치의 경우 MAC 어드레스에 따라 스위칭하기 때문에 다른 컴퓨터의 MAC 어드레스를 사용할 경우 문제가 생길 소지가 있다. 그러나, MAC 어드레스의 변화를 감지하는 호스트 또는 침입감지시스템(IDS)이나 방화벽(Firewall) 등이 존재할 경우에는 이렇게 자기 자신의 MAC 어드레스를 사용할 수 없을 경우도 있으나, 이 때에는 해당 NIDS나 방화벽(Firewall)에서 그 기능을 제거하고 사용할 수 있다.

셋째는 임의외 MAC 어드레스를 사용하는 경우로, 특수한 목적 또는 필요에 의해 특정한 MAC 어드레스를 사용해야만 하는 경우이다. 이 때는 사용할 MAC 어드레스를 지정해 주어야 한다.

RN이 패킷(Packet)을 보낼 때 사용하는 목적지 MAC주소는 크게 세 가지 이다. 첫째는 원래의 MAC 어드레스를 사용하는 경우로, 이 경우는 더미 허브(Dummy Hub)에 연결되어 있는 경우이다. 더미 허브는 MAC 어드레스에 의해 아무런 영향을 받지 않기 때문에, IP 주소에 대응하는 MAC 어드레스를 사용하여도 상관이 없다. 따라서, 부작용이 전혀 없도록 원래의 MAC 어드레스를 사용하는 것이 가장 좋은 방법이다.

둘째는 응답 게이트웨이(Response Gateway)의 MAC 어드레스를 사용하는 경우로, 응답 게이트웨이를 설정할 경우 IP 주소를 이더넷 주소로 변환하기 위한 사상(Mapping)을 처리하는 ARP(Address Resolution Protocol) 정보를 처리하도록 해야하며, 여기서 얻어진 게이트웨이의 MAC 어드레스를 목적지 MAC 어드레스로 사용하여 패킷을 전송하게 된다.

셋째는 임의의 MAC 어드레스를 사용하는 경우로, 특수한 목적 또는 필요에 의해 특정한 MAC 어드레스를 사용해야만 하는 경우이다. 이 때는 사용할 MAC 어드레스를 지정해 주어야 한다.

본 발명에서 여러개의 모니터링 NIC이 트래픽(Traffic) 분석을 수행하고 있을 경우, 여러 개의 모니터링 NIC이 각각 응답 NIC을 하나씩 가지게 된다. 이 경우에 하나의 응답 NIC이 여러개의 모니터링 NIC에 대해 설정될 수 있으므로, 각각의 응답 NIC은 한개 이상의 모니터링 NIC에 대해 응답 MAC 어드레스를 결정하는 설정정보를 가지고 있어야 한다.

응답을 다루는 모듈은 그에 관련된 모든 모니터링 NIC에 대한 MAC 어드레스 선택 모드를 가지며, 응답 요청이 들어왔을 때, 해당 응답이 어떤 MAC 어드레스를 사용해야 하는지를 결정하게 된다. 이는 어떤 모니터링 NIC을 경유하여 들어온 트래픽(Traffic) 인지를 같이 넘겨줌으로써 MAC 어드레스를 결정하게 된다.

도 4 는 본 발명에 따른 네트워크 침입감시 시스템의 설정 프로그램 개요도이다.

모듈(n) 매니저를 초기화 할때 각자의 세팅(Setting)을 설정 파일(File) 또는 레지스트리(Registry)로부터 읽어들여서 사용할 NIC(n) 인스턴스(Instance)를 초기화 시킬 때, 그 값들에 따라 필요한 정보들을 기록한다. 이 기록된 정보들에 의하여 모듈(n) 매니저로부터 패킷을 보내겠다는 요청이 있을 시, 해당하는 NIC(n) 인스턴스가 어떠한 하드웨어 주소를 사용하여 패킷을 보낼 수 있는지를 판단하고 요청된 응답을 수행하게 된다.

따라서, 상기와 같이 함에 의해 네트워크 장비의 제한 때문에 해킹에 대해 적절히 조치하지 못하는 일을 최소화 할 수 있으며, 동시에 여러개의 네트워크를 감시해야하는 상황하에서도 정확하게 감시 작업할 수 있는 등의 본 발명의 목적을 달성할 수 있게 된다.

발명의 효과

이상에서 설명한 바와같은 본 발명에 따른 네트워크 침입감시 시스템은 네트워크 관련 하드웨어의 한계를 극복하여 해킹이나 서비스 공격, 스캐닝 등의 네트워크 침입을 감지했을 때, 네트워크의 구성이 어떻게 되어 있는지에 상관없이 해킹 시도에 대해 능동적으로 대처할 수 있어 해킹에 대해 적절히 조치하지 못하는 일을 최소화 할 수 있으며, 동시에 여러개의 네트워크를 감시해야하는 상황하에서도 정확하게 감시할 수 있는 유용한 효과를 가진다.

본 발명은 첨부된 도면을 참조하여 바람직한 실시예를 중심으로 기술되었지만 당업자라면 이러한 기재로부터 후술하는 특허청구범위에 의해 포괄되는 본 발명의 범주를 벗어남이 없이 다양한 변형이 가능하다는 것은 명백하다.

(57) 청구의 범위

청구항 1.

네트워크에 흐르는 모든 트래픽(Traffic)을 분석하여 위험하거나, 위험 가능성이 있는 행위들을 탐지하여 이를 네트워크 액티비티(SNA) 및 세션 킬(Session Kill)을 수행하여 해킹을 차단 및 방지하는 네트워크 침입탐지 시스템(NIDS : Network Based Intrusion Detection System)에 있어서,

상기 네트워크 침입탐지 시스템(NIDS)이:

네트워크로부터 분석대상 트래픽의 패킷을 수집하는 모니터링 NIC과;

네트워크로 네트워크 액티비티(SNA) 및 세션 킬(Session Kill)을 수행하기 위한 패킷을 보내는 응답 NIC을;

포함하는 적어도 하나 이상의 제 1 형의 네트워크 인터페이스 카드를 포함하는 것을 특징으로 하는 네트워크 침입탐지 시스템.

청구항 2.

제 1 항에 있어서,

상기 네트워크 침입탐지 시스템(NIDS)이:

네트워크로부터 분석대상 트래픽의 패킷을 수집하는 모니터링 NIC 만으로 이루어진 적어도 하나 이상의 제 2 형의 네트워크 인터페이스 카드를 더 포함하는 것을 특징으로 하는 네트워크 침입탐지 시스템.

청구항 3.

제 2 항에 있어서,

상기 제 2 형의 네트워크 인터페이스 카드는:

상기 제 1 형의 네트워크 인터페이스 카드의 응답 NIC 중 어느 하나를 공유하되, 해당 응답 NIC은 공유된 제 2 형의 네트워크 인터페이스 카드의 네트워크로의 응답에 대한 환경정보를 포함함에 의해 상기 제 2 형의 네트워크 인터페이스 카드의 모니터링 NIC이 수집한 패킷에 대한 응답 패킷을 상기 공유된 응답 NIC을 통해 네트워크로 보내는 것을 특징으로 하는 네트워크 침입탐지 시스템.

청구항 4.
제 1 항 또는 제 2 항 또는 제 3 항 중의 어느 한 항에 있어서,

상기 네트워크 침입탐지 시스템이:

상기 적어도 하나 이상의 응답 NIC으로부터 네트워크로 전송되는 네트워크 액티비티(SNA) 및 세션 킬(Session Kill)을 수행하기 위한 패킷들을 라우팅(Routing)하는 응답 게이트웨이(Gateway)를 더 포함하는 것을 특징으로 하는 네트워크 침입탐지 시스템

청구항 5.
제 1 항 또는 제 2 항 또는 제 3 항 중의 어느 한 항에 있어서,

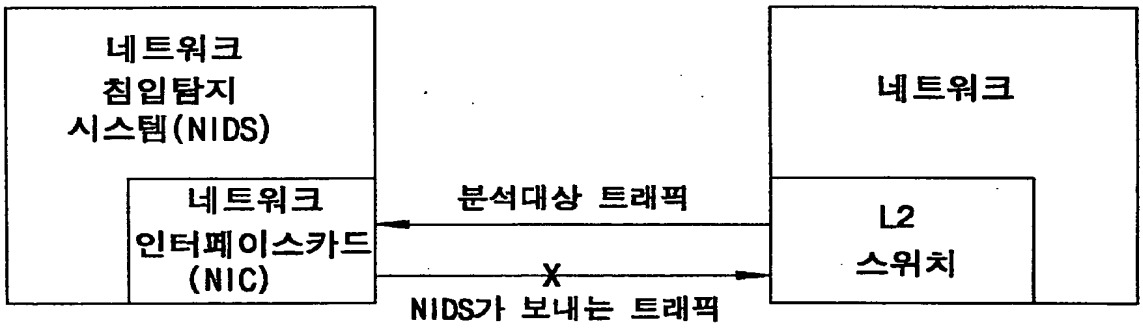
상기 제 1 형의 네트워크 인터페이스카드의 모니터링 NIC과 응답 NIC이 일체인 것을 특징으로 하는 네트워크 침입탐지 시스템.

청구항 6.
제 1 항 또는 제 2 항 또는 제 3 항 중의 어느 한 항에 있어서,

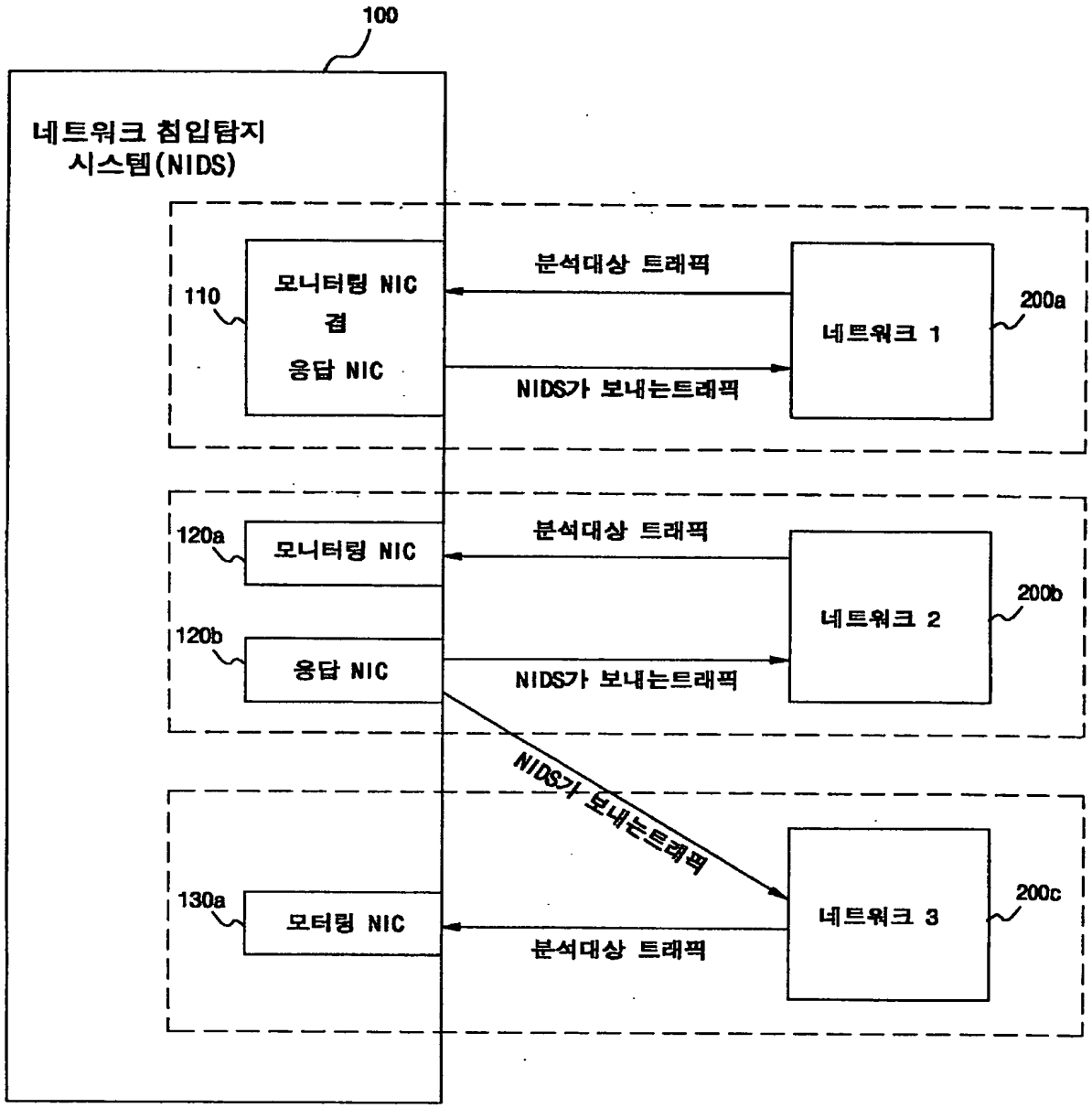
상기 제 1 형의 네트워크 인터페이스카드의 모니터링 NIC과 응답 NIC이 각각 분리되어 구성된 것을 특징으로 하는 네트워크 침입탐지 시스템.

도면

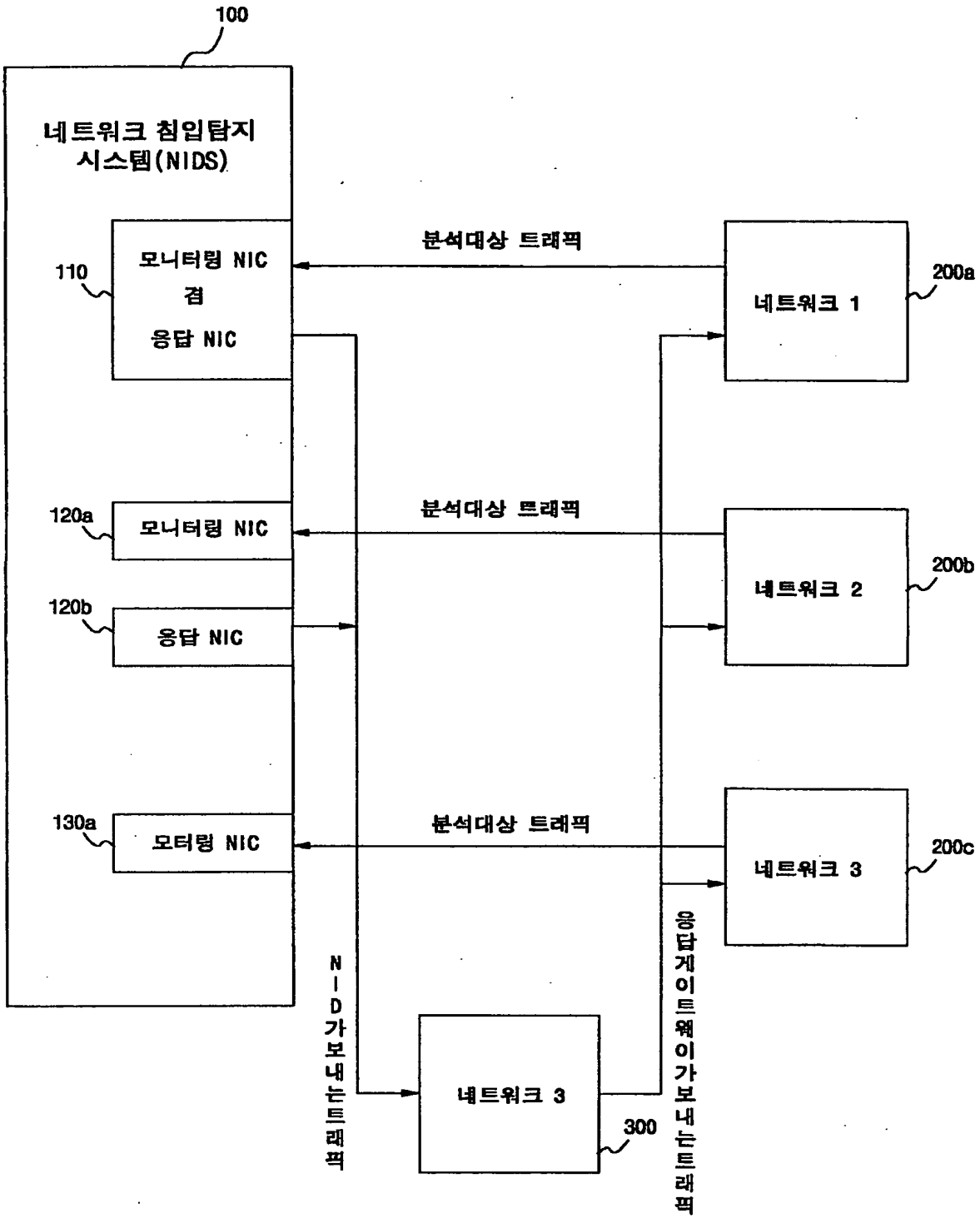
도면 1



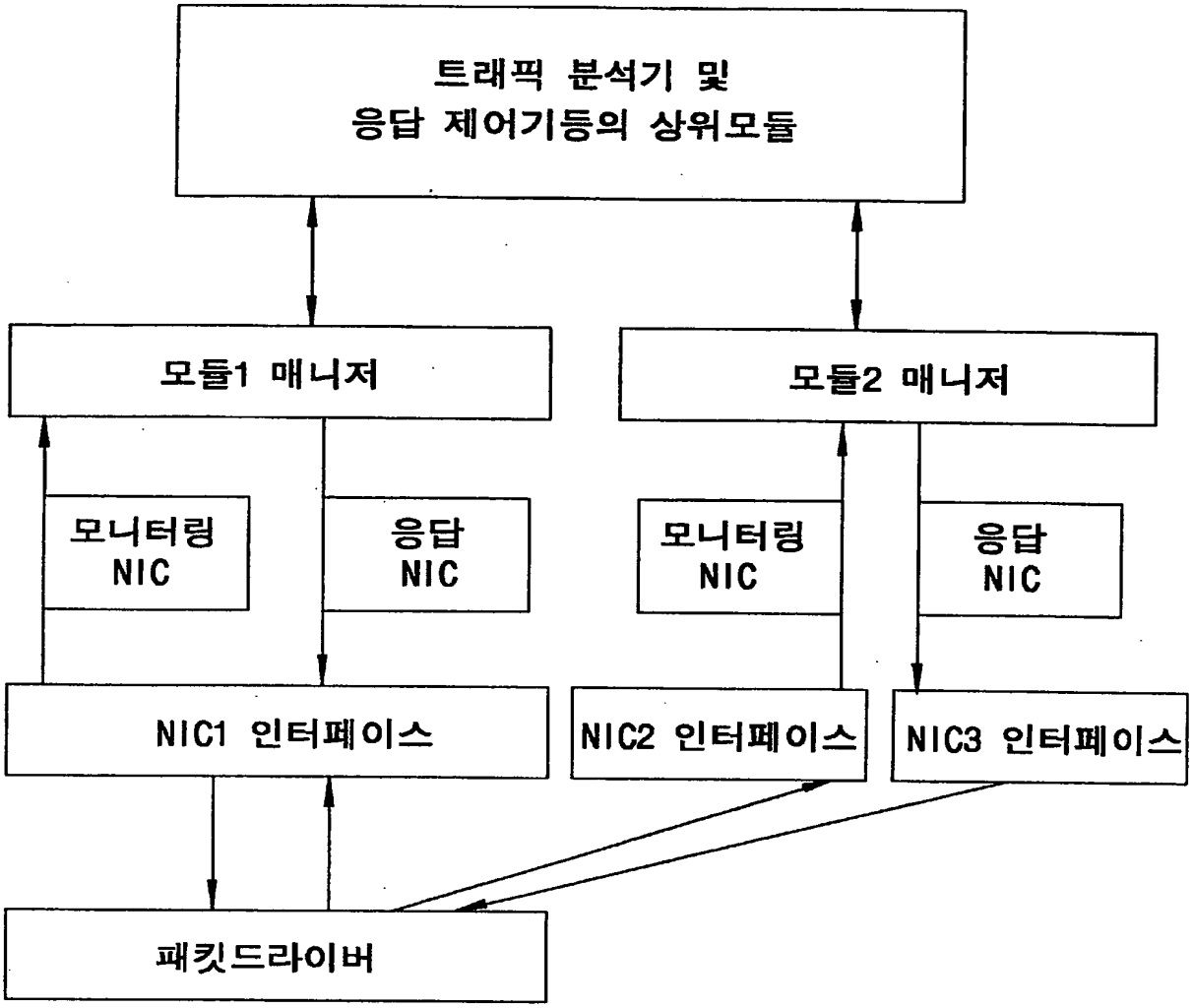
도면 2


100
네트워크 침입탐지
시스템(NIDS)
110
모니터링 NIC
겸
응답 NIC
분석대상 트래픽
NIDS가 보내는트래픽
네트워크 1
200a
120a
모니터링 NIC
120b
응답 NIC
분석대상 트래픽
NIDS가 보내는트래픽
네트워크 2
200b
NIDS가 보내는트래픽
130a
모터링 NIC
분석대상 트래픽
네트워크 3
200c

도면 3


100
네트워크 침입탐지 시스템(NIDS)
110
모니터링 NIC 겸 응답 NIC
120a
모니터링 NIC
120b
응답 NIC
130a
모터링 NIC
분석대상 트래픽
분석대상 트래픽
분석대상 트래픽
네트워크 1
200a
네트워크 2
200b
네트워크 3
200c
N-D가보내는트래픽
네트워크 3
300
응답게이트웨이가보내는트래픽

도면 4


트래픽 분석기 및
응답 제어기등의 상위모듈
모듈1 매니저
모듈2 매니저
모니터링
NIC
응답
NIC
모니터링
NIC
응답
NIC
NIC1 인터페이스
NIC2 인터페이스
NIC3 인터페이스
패킷드라이버